ID: 680484
Sample Name: SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Cookbook: default.jbs
Time: 17:21:01
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

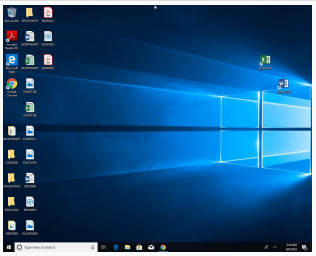
Windows Analysis Report

SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe

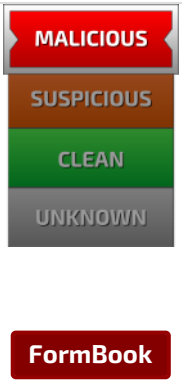
Overview

General Information

Sample Name:	SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Analysis ID:	680484
MD5:	47b96215204bad.
SHA1:	6b5af0c13af653e..
SHA256:	613edebe9f20eff..
Tags:	exe
Infos:	



Detection



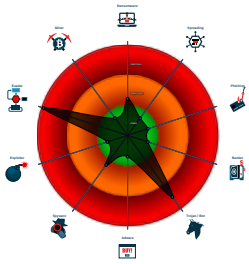
FormBook

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Uses netstat to query active networ…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe (PID: 5860 cmdline: "C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe" MD5: 47B96215204BAD8DB8CE43A4685EE74C)
  - SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe (PID: 5032 cmdline: C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe MD5: 47B96215204BAD8DB8CE43A4685EE74C)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 5260 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.classicpretty.com/qkkr/"
  ],
  "decoy": [
    "7gCdEvi4PU1csVn41UdG95Ufy7SR",
    "3/kS/9ZgObTlShULwBM8",
    "UmkOiGYioBlRs12D06oGbv8X",
    "JHVcqPzZQM4=",
    "597t26RTZoSV64ak89Q0kUqhiRWZ",
    "EGeQhlYOeLg5jSU=",
    "uPMS7r10aXmis6FQ",
    "bBxVPrS1SNM=",
    "TGkjh14+21mDz2aAy6gGbv8X",
    "Jm3QiEjsOJLnDPGK/GhezP9J+w==",
    "nqvLrZVqboJ018dvX1tvKr8fy7SR",
    "6TLsXCjsdIRapiVFFW8QLq/Jpyz84bgt",
    "zAmlDcFiMH2BzqHdfrG10w==",
    "80byQOwlybg5jSU=",
    "7+wUCuhxEmJpdn22IQ==",
    "2BtALhSuf7+qDZLEoxy5YDqSQ7Y=",
    "Sl3pWETqy+UJZw==",
    "5O597tysPrbdIcfwRTbC6zqSQ7Y=",
    "jLnMq5lBKkZChXBmO5s=",
    "kYuyrH0QySmG5nu1XpW42Q==",
    "AVBMJBLacrg5jSU=",
    "A3EiigAN5iQV",
    "F/sA6K0zGK38TcjqqZf6a/EO",
    "mO3ly4UvKJ/lKazOfrG10w==",
    "g5r8xzg9f6x0bHBmO5s=",
    "/iOw+dqWvwIJZTvwt5b2X+QE",
    "VpOyflNVFjEf",
    "GXQWhGozhjmnBet72T7lWsEQ8w==",
    "rdYUAOqoZ7nfIslcROQt2fE=",
    "X2RvVx7e62F4x5E4CnV6WsEQ8w==",
    "0yCtNg7Wcrg5jSU=",
    "mbPTqHUVyhQpm3BmO5s=",
    "+kM7JyLOqy5x0YEX4FFtWsEQ8w==",
    "zzzpWjjD3j6BlWuc/uL7qEOX+qaI",
    "txIhBcxwTa3+XYzyzJUw2w==",
    "UVf1TAGb+4XmRb/87Vn5I6DHK9Gb",
    "NpNAvptlQJ8D2yU3Ft/6a/EO",
    "4w0O8uNWqzaZ6lNzR+Qt2fE=",
    "T0/XSzLua7BYvzw=",
    "AQCJ9bFtcX+S2KNXKQ==",
    "S6XAupU+A01SrXBmO5s=",
    "WJvBvpRANTlylxBBJRQj",
    "Roespn0fNnSis6FQ",
    "Zl5zgV8FJGthukV331t6WsEQ8w==",
    "yR+1GPuz6jBXvZc8CfH5tWXFZft+h3kl",
    "GEdYQw64y+UJZw==",
    "V1FZLCjxcvJZsZ5efrG10w==",
    "8xE8RCS8y+UJZw==",
    "gdDo2JE7Q8srfuoAw6z6a/EO",
    "ywKjBNd8tKn2FbvOfrG10w==",
    "MdAFl1EPS0heyzI=",
    "SZOLcznb1vDhGNuKX1F4F8r4lqQvvQ==",
    "8RIpGwG+nyBWdn22IQ==",
    "vxU/Ngu8y+UJZw==",
    "c5C7l14L4DFQdn22IQ==",
    "vAftT7Dd5+yadn22IQ==",
    "aLlEn2PsEmiis6FQ",
    "2yHKQhapTpn2LLNH",
    "vLhJvJ5k516vEb73TypG4pEfy7SR",
    "k+Hy17lycX+S2KNXKQ==",
    "0NHXxJo7WJqhGrDmvK36a/EO",
    "3tQjHQW5y+UJZw==",
    "Yu0MIIV4OYT2LLNH",
    "aK05uHh9U9cgfg=="
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0xdc40:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x6e27:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x6c25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x66d1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x6d27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x6e9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x58ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xc897:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xd9aa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x92e9:$sqlite3step: 68 34 1C 7B E1 • 0x941c:$sqlite3step: 68 34 1C 7B E1 • 0x932b:$sqlite3text: 68 38 2A 90 C5 • 0x9473:$sqlite3text: 68 38 2A 90 C5 • 0x9342:$sqlite3blob: 68 53 D8 7F 8C • 0x9495:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000000.460111933.0000000000401000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x57e1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1ce40:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x977f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16027:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
6.0.SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x15e25:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x158d1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15f27:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1609f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x934a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14aec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa092:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ba97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cbaa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x184e9:$sqlite3step: 68 34 1C 7B E1 • 0x1861c:$sqlite3step: 68 34 1C 7B E1 • 0x1852b:$sqlite3text: 68 38 2A 90 C5 • 0x18673:$sqlite3text: 68 38 2A 90 C5 • 0x18542:$sqlite3blob: 68 53 D8 7F 8C • 0x18695:$sqlite3blob: 68 53 D8 7F 8C
15.2.NETSTAT.EXE.3a67a24.3.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Click to see the 5 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

Uses netstat to query active network connections and open ports

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

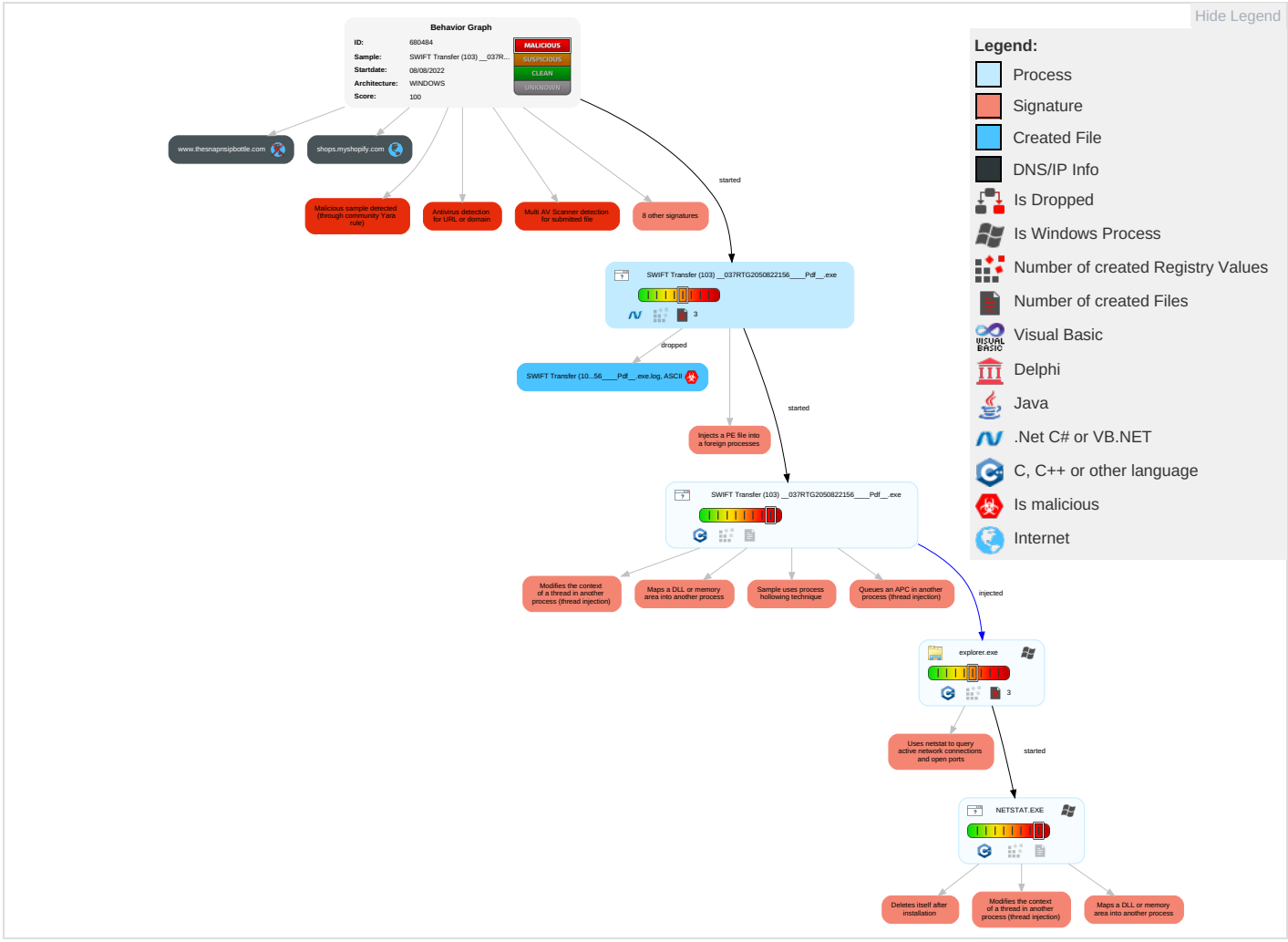
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	5 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	1 System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Connections Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe	40%	Virustotal		Browse
SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe	46%	ReversingLabs	Win32.Spyware.Noon	
SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
shops.myshopify.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
www.classicpretty.com/qkkr/	1%	Virustotal		Browse
www.classicpretty.com/qkkr/	100%	Avira URL Cloud	malware	
http://boards.4chan.org3Retrieving	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shops.myshopify.com	23.227.38.74	true	false	• 0%, Virustotal, Browse	unknown
www.thesnapnsipbottle.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.classicpretty.com/qkkr/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://boards.4chan.org/b/	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe	false		high
http://www.fontbureau.com/designers?	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://boards.4chan.org3Retrieving	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://images.4chan.org/	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe	false		high
http://www.urwpp.deDPlease	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SWIFT Transfer (103) __037RTG2050822156_ ___Pdf__.exe, 00000000.00000002.47969027 3.00000000071E2000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680484
Start date and time: 08/08/202217:21:01	2022-08-08 17:21:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/1@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 91.8% (good quality ratio 78.4%) • Quality average: 70.5% • Quality standard deviation: 34.4%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:22:25	API Interceptor	1x Sleep call for process: SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe.log

Process:	C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.461302452992026
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
File size:	988160
MD5:	47b96215204bad8db8ce43a4685ee74c
SHA1:	6b5af0c13af653e5347e1b5e6a7f3bbecee257d5
SHA256:	613edebe9f20eff6958bc447fa000388c1b986e1cdb76930ca061d2c92fe952c
SHA512:	b52c7e468cce2953a3d4880d1b2f8dc147147c8311c6f79b6bd766b67b7f4a1b28f34498bc02341cdcac0a735ecf8d6e78e495991780aa0d72f2acfe4f30f47e
SSDEEP:	24576:n6n08/X7tViZ4mMvQQdC6BTe9IbUDHDlF:n6n08/X7tM4m+QQb7UT
TLSH:	86259D07AFA43705E4B75BB9DD5B686183F27809717EE3782E905C9B2DFA301D80162B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....r.b.....0..:.....E... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	c68ce86ecc8c8ac8

Static PE Info

General

Entrypoint:	0x4e45e6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F072E8 [Mon Aug 8 02:20:24 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
mov bh, 1Dh
rol dword ptr [esi+ebp*2], 3Bh
or byte ptr [ecx], FFFFFFD9h
inc ebx
or eax, 130476DCh
imul ebp, dword ptr [ebx-3Bh], 17h
mov dl, 4Dh
xchg byte ptr [edx], bl
add eax, B81E4750h
in eax, dx

Instruction
or byte ptr [esi], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe4594	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe6000	0xd4bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe3964	0xe3a00	False	0.7369566429846238	data	7.5981105192888725	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0xd4bc	0xd600	False	0.27655884929906543	data	3.7576742623203367	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf4000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe6128	0x94a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xef5e0	0x25a8	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xf1b98	0x10a8	data		
RT_ICON	0xf2c50	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf30c8	0x3e	data		
RT_VERSION	0xf3118	0x3a0	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:24:22.907291889 CEST	63301	53	192.168.2.5	8.8.8.8
Aug 8, 2022 17:24:22.943212032 CEST	53	63301	8.8.8.8	192.168.2.5

DNS Queries

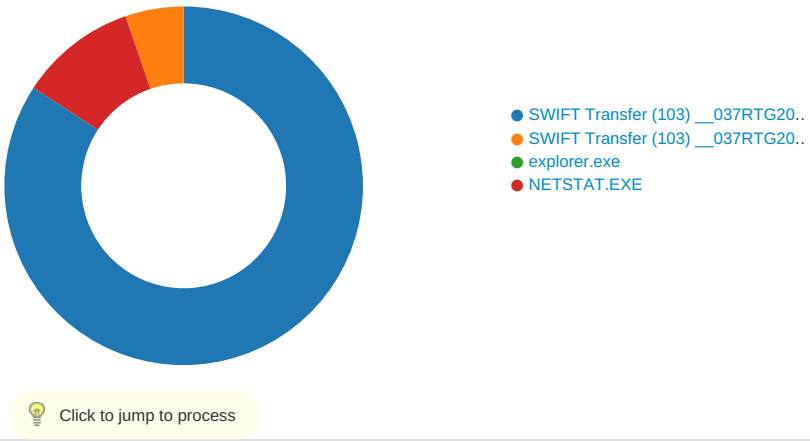
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:24:22.907291889 CEST	192.168.2.5	8.8.8.8	0xa5c5	Standard query (0)	www.thesnapnsipbottle.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:24:22.943212032 CEST	8.8.8.8	192.168.2.5	0xa5c5	No error (0)	www.thesnapnsipbottle.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:24:22.943212032 CEST	8.8.8.8	192.168.2.5	0xa5c5	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe PID: 5860, Parent PID: 5696

General

Target ID:	0
Start time:	17:22:06
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe"
Imagebase:	0xd10000
File size:	988160 bytes
MD5 hash:	47B96215204BAD8DB8CE43A4685EE74C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.467346210.00000000032FB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.474529782.000000000436D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.474529782.000000000436D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.474529782.000000000436D000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.474529782.000000000436D000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.473127141.000000000354B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe PID: 5032, Parent PID: 5860

General

Target ID:	6
Start time:	17:22:27
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe
Imagebase:	0x850000
File size:	988160 bytes
MD5 hash:	47B96215204BAD8DB8CE43A4685EE74C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.460111933.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.460111933.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.460111933.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.460111933.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41B2F7	NtReadFile

Analysis Process: explorer.exe PID: 684, Parent PID: 5032

General

Target ID:	7
Start time:	17:22:33
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.607026478.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.566602114.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.566602114.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.566602114.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.566602114.000000000DE02000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: **5260**, Parent PID: **684**

General

Target ID:	15
Start time:	17:23:44
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x90000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.689373847.0000000000110000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.689373847.0000000000110000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.689373847.0000000000110000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.689373847.0000000000110000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.693653140.0000000003260000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.693653140.0000000003260000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.693653140.0000000003260000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.693653140.0000000003260000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.693445198.0000000002F60000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000002.693445198.0000000002F60000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.693445198.0000000002F60000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.693445198.0000000002F60000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SWIFT Transfer (103) __037RTG2050822156____Pdf__.exe	success or wait	1	327B327	NtDeleteFile

File Path	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	327B2F7	NtReadFile

Disassembly

No disassembly